

Japanese Patent Laid-open No. 2003-46973 A

Publication date : Feb. 14, 2003

Applicant : Nippon Hoso Kyokai

Title : SCRAMBLING METHOD, TRANSMISSION METHOD,

5 TRANSMISSION APPARATUS, AND RECEIVER.

[0050] Furthermore, according to the present invention,  
an update of the scramble key used in scrambling is  
performed in synchronization with a coding unit of signals,  
10 or with a unit of at least one GOP (Group Of Picture).  
Accordingly, the scramble key in subject sections can be  
clearly identified, and the descrambling at the time of  
special reproductions can be easily performed.

15 [0070] Fig. 4 is one example of an embodiment of the  
present invention.

[0085] While the number of the Ks in the ECM is three in  
the explanation of the present invention, the allocated  
20 number of the Ks is not limited thereto.

[Fig. 4]

One example of embodiment of the present invention

25 Section I

Section II

Section III

Section IV

30 TS packet and its encryption key

TS packet

(Odd number 1)

(Even number 1)

**THIS PAGE BLANK (USPTO)**

(Odd number 2)  
(Even number 2)

Keys in ECM transferred between each section

5 (Odd number 1)  
(Even number 1)  
(Even number 0)

(Odd number 2)  
10  
(Even number 2)

(Odd number 3)

15 Time

**THIS PAGE BLANK (USPTO)**

**THIS PAGE BLANK (USPTO)**

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-46973

(P2003-46973A)

(43)公開日 平成15年2月14日(2003.2.14)

(51)IntCl.<sup>7</sup>

H 0 4 N 7/167

7/16

識別記号

F I

H 0 4 N 7/16

7/167

テ-マコ-ト\*(参考)

Z 5 C 0 6 4

Z

審査請求 未請求 請求項の数12 O L (全 12 頁)

(21)出願番号 特願2001-232023(P2001-232023)

(22)出願日 平成13年7月31日(2001.7.31)

(71)出願人 000004352

日本放送協会

東京都渋谷区神南2丁目2番1号

(72)発明者 難波 誠一

東京都世田谷区砦一丁目10番11号 日本放送協会 放送技術研究所内

(72)発明者 木村 武史

東京都世田谷区砦一丁目10番11号 日本放送協会 放送技術研究所内

(74)代理人 100070150

弁理士 伊東 忠彦

Fターム(参考) 5C064 BA01 BB02 BC07 BC17 CA14

CB01

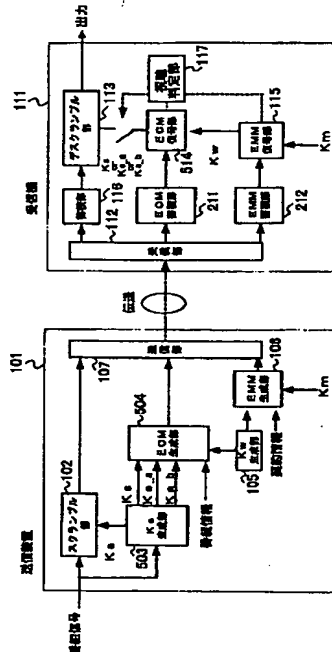
(54)【発明の名称】 スクランプル方法、送信方法、送信装置、及び受信機

(57)【要約】

【課題】 スクランプルされた伝送信号において、デスクランブルしながら早送り、巻き戻し等の特殊再生を可能とする信号のスクランブル方法、送信方法、送信装置、及び受信機に関する。

【解決手段】 本発明は、番組の映像や音声等の信号を区間に分割し、その区間毎に異なるスクランブル鍵 $K_s$ を用いてスクランブルを行う際に、前記スクランブルを復元するための関連情報(ECM)に含まれる $K_s$ の数を従来よりも増やすことにより、早送り、巻き戻し等の特殊再生時に受信者が認識可能となる映像信号及び音声信号を表示可能とする。

本発明を使用した限定受信システムの一構成例



## 【特許請求の範囲】

【請求項 1】 スクランプル鍵を生成する鍵生成段階と、  
前記鍵生成段階によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル段階と、  
スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成段階とを有するスクランブル方法において、  
前記スクランブル鍵情報生成段階において生成されたスクランブル鍵情報は、既に使用したスクランブル鍵に関するスクランブル鍵情報を有することを特徴とするスクランブル方法。

【請求項 2】 スクランプル鍵を生成する鍵生成段階と、  
前記鍵生成段階によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル段階と、  
スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成段階とを有するスクランブル方法において、  
前記スクランブル鍵情報生成段階において生成されたスクランブル鍵情報は、  
現在の区間の信号のスクランブルに使用するスクランブル鍵と、  
隣接する次の区間の信号のスクランブルに使用するスクランブル鍵と、  
隣接する 1 つ前の区間の信号のスクランブルに使用するスクランブル鍵とに関する情報を少なくとも有することを特徴とするスクランブル方法。

【請求項 3】 スクランプル鍵を生成する鍵生成段階と、  
前記鍵生成段階によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル段階とを有するスクランブル方法において、  
前記スクランブル段階は、スクランブル時に用いられるスクランブル鍵の更新を、信号の符号化単位に同期して行うことを特徴とするスクランブル方法。

【請求項 4】 請求項 3 記載のスクランブル方法において、  
前記スクランブル段階は、スクランブル時に用いられるスクランブル鍵の更新を、符号化信号の少なくとも 1 つの GOP 単位に同期して行うことを特徴とするスクランブル方法。

【請求項 5】 請求項 3 又は 4 記載のスクランブル方法により生成されたスクランブル信号と暗号化されたスクランブル鍵情報とを同時に送信する送信方法において、  
前記スクランブル鍵情報は、符号化単位に同期して区切られた信号の切り替え点における直前もしくは直後、又はその両方に付加することを特徴とする送信方法。

【請求項 6】 スクランプル鍵を生成する鍵生成部と、  
前記鍵生成部によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル部と、  
スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成部とを有する送信装置において、  
前記スクランブル鍵情報生成部において生成されたスクランブル鍵情報は、既に使用したスクランブル鍵に関するスクランブル鍵情報を有することを特徴とする送信装置。

【請求項 7】 スクランプル鍵を生成する鍵生成部と、  
前記鍵生成部によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル部と、  
スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成部とを有する送信装置において、  
前記スクランブル鍵情報生成部において生成されたスクランブル鍵情報は、  
現在の区間の信号のスクランブルに使用するスクランブル鍵と、  
隣接する次の区間の信号のスクランブルに使用するスクランブル鍵と、  
隣接する 1 つ前の区間の信号のスクランブルに使用するスクランブル鍵とに関する情報を少なくとも有することを特徴とする送信装置。

【請求項 8】 スクランプル鍵を生成する鍵生成部と、  
前記鍵生成部によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル部とを有する送信装置において、  
前記スクランブル部は、スクランブル時に用いられるスクランブル鍵の更新を、信号の符号化単位に同期して行うことを特徴とする送信装置。

【請求項 9】 請求項 8 記載の送信装置において、  
前記スクランブル部は、スクランブル時に用いられるスクランブル鍵の更新を、符号化信号の少なくとも 1 つの GOP 単位に同期して行うことを特徴とする送信装置。

【請求項 10】 請求項 8 又は 9 記載の送信装置により生成されたスクランブル信号と暗号化されたスクランブル鍵情報とを同時に送信する送信装置において、  
前記スクランブル鍵情報は、符号化単位に同期して区切られた信号の切り替え点における直前もしくは直後、又はその両方に付加することを特徴とする送信装置。

【請求項 11】 スクランプル鍵によりスクランブルされた信号を受信する受信部と、  
スクランブル信号を蓄積する蓄積部と、  
スクランブル鍵情報を復号するスクランブル鍵情報復号部と、

スクランブル信号をデスクランブルするデスクランブル

部とを有する受信機において、  
前記スクランブル鍵情報復号部において復号されたデスクランブル鍵情報は、既に使用したデスクランブル鍵に関するデスクランブル鍵情報を有することを特徴とする受信機。

【請求項 12】 スクランブル鍵によりスクランブルされた信号を受信する受信部と、  
スクランブル信号を蓄積する蓄積部と、  
スクランブル鍵情報を復号するスクランブル鍵情報復号部と、  
スクランブル信号をデスクランブルするデスクランブル部とを有する受信機において、  
前記スクランブル鍵情報復号部において復号されたデスクランブル鍵情報は、  
現在の区間の信号のデスクランブルに使用するデスクランブル鍵と、  
隣接する次の区間の信号のデスクランブルに使用するデスクランブル鍵と、  
隣接する 1 つ前の区間の信号のデスクランブルに使用するデスクランブル鍵とに関する情報を少なくとも有することを特徴とする受信機。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】スクランブル方法、送信方法、送信装置、及び受信機に関する。

【0002】

【従来の技術】放送サービスを伝送する電波は誰でも受信することができる。このため、電波が受信できても番組やサービスの内容が判別できないように情報を秘匿する処理を行っている。これは一般にスクランブルと呼ばれている。

【0003】ところで、記録された信号を再生し視聴する場合において、特に早送りや巻き戻しを行う、いわゆる特殊再生機能を要する場合、従来技術ではスクランブルが行われていない状態（受信側においては、デスクランブルされた状態）で記録するため、アナログ信号と同様に、ある程度までの速度範囲であれば、内容が理解できるような画質の再生を可能にしていた。

【0004】しかし、例えば、ペーパービュー（以下 PPV とする）方式による番組のような場合、デスクランブルを行う時に課金処理が行われるため、一時的に種々の番組を記録しておき、希望する時間にそれらから選択して番組を視聴するといういわゆるホームサーバーとして利用するような状況では、最終的には見ない番組にも課金されてしまうという問題がある。

【0005】ここで、前記の内容を図を用いて説明する。

【0006】図 1 は、従来の限定受信システムの第一の構成例である。

【0007】図 1 において、従来の限定受信システムは

送信装置 101、及び受信機 111 より構成されている。

【0008】送信装置 101 は、スクランブル部 102、Ks（スクランブル鍵）生成部 103、ECM 生成部 104、Kw（ワーク鍵）生成部 105、EMM 生成部 106、送信部 107 より構成されている。

【0009】また、受信機 111 は、受信部 112、デスクランブル部 113、ECM 復号部 114、EMM 復号部 115、蓄積部 116、視聴判定部 117 より構成されている。

【0010】送信装置 101 に番組信号が入力されると、スクランブル部 102 は Ks を用いて番組信号をスクランブルする。Ks 生成部 103 は、スクランブル部 102 及び ECM 生成部 104 に同一の Ks を出力する。ECM 生成部 104 は、Ks 及び番組の種類や時刻、視聴料金等の属性情報（以下 番組情報 とする）を Kw を用いて暗号化し、ECM（Entitlement Control Message）を生成する。Kw 生成部 105 は、ECM 生成部 104 及び EMM 生成部 106 に同一の Kw を出力する。EMM 生成部 106 は、Kw 及び受信者の契約したチャンネル、又は契約有効期限等の契約内容の情報（以下 契約情報 とする）を、Km（マスタ鍵）を用いて暗号化を行い、EMM（Entitlement Management Message）を生成する。送信部 107 は、スクランブル信号、ECM、EMM を送信する。

【0011】受信機 111 は伝送されたスクランブル信号を受信部 112 が受け取り、スクランブル信号はデスクランブル部 113 へ、ECM 信号は ECM 復号部 114 へ、EMM 信号は EMM 復号部 115 へ出力される。

【0012】EMM 復号部 115 は予め与えられている Km を用いて EMM の復号を行う。ECM 復号部 114 は EMM 復号部 115 で取得された Kw を用いて復号を行う。視聴判定部 117 は、EMM 復号部 115 にて復号された契約情報と ECM 復号部 114 にて復号された番組信号とを用いて、受信したスクランブル信号が受信者との契約上視聴可能な信号であるかを判定し、視聴可能であった場合、取得された Ks をデスクランブル部 113 に与えてデスクランブルを行う。これら ECM 復号部 114、EMM 復号部 115、及び視聴判定部 117 は、CPU（Central Processing Unit）内蔵の IC（Integrated Circuit）カードの中の処理プログラムとして実現されることも多い。デスクランブルされた信号は蓄積部 116 に蓄積され、特殊再生を含む再生が行われる。

【0013】番組信号が送信装置 101 に入力されると、スクランブル部 102 は Ks 生成部 103 から入力された Ks を用いてスクランブルを行い、送信部 107 へ出力する。Ks は番組情報と共に ECM 生成部 104 へ入力する。ECM 生成部 104 は、Ks と番組情報とから ECM を生成し、Kw 生成部 105 より入力された

Kwを用いて暗号化した後、送信部107へ出力する。なお、Ksは従来技術においては、時間単位（1秒程度）で更新されている。また、KwはECMの暗号を解読するために必要な鍵であり、1ヶ月～1年程度で更新を行うよう想定されている。Kwは契約情報と共にEMM生成部106に入力し、Kwと契約情報とからEMMを生成し、Kmを用いて暗号化した後、送信部107へ出力する。送信部107は、スクランブル信号、ECM、EMMを送信する。

【0014】受信機111では、伝送信号を受信部112で受信し、スクランブル信号をデスクランブル部113へ、ECMをECM復号部114へ、EMMをEMM復号部115へ出力する。その後、EMM復号部115でKmを用いてEMMの復号を行い、契約情報及びKwを取得する。ECM復号部114はEMM復号部115から入力されたKwを用いて復号を行い、Ks及び番組情報を取得する。

【0015】ここで、先ほどEMM復号部115にて復号された契約情報とECM復号部114にて復号された番組信号とから、受信信号が受信者にとって視聴可能な信号であるかを視聴判定部117で判定し、視聴可能な信号であった場合、デスクランブル部113にKsを送り、スクランブル信号のデスクランブルを行う。デスクランブルされた信号は、蓄積部116で蓄積され、受信者の希望する出力方法で出力する。従来のシステムでは、デスクランブルされた信号が蓄積されているため、早送り、巻き戻し等の特殊再生も可能となる。

【0016】しかしながら、PPV方式による番組のような場合、デスクランブルを行う時に課金処理が行われるため、蓄積部116に蓄積した信号は、受信者が視聴しない場合においても、既に課金されていることになる。

【0017】そこで次に、受信者が視聴した番組だけが課金されるようにした従来の限定受信システムの第二の構成例を図2に示す。

【0018】図2において、従来の限定受信システムは送信装置101、及び受信機111より構成されている。送信装置101は、スクランブル部102、Ks生成部103、ECM生成部104、Kw生成部105、EMM生成部106、送信部107より構成されている。また、受信機111は、受信部112、デスクランブル部113、ECM復号部114、EMM復号部115、蓄積部116、視聴判定部117、ECM蓄積部211、EMM蓄積部212より構成されている。

【0019】図2の限定受信システムにおける送信装置101の動作内容は、図1の送信装置101と同様であるため、説明を省略する。

【0020】受信機111において、伝送信号を受信部112で受信し、スクランブル信号を蓄積部116へ、ECMをECM蓄積部211へ、EMMをEMM蓄積部

212へ出力する。蓄積部116にはスクランブルされたままの信号が蓄積される。EMM蓄積部212は、EMM信号を復号せずにそのまま蓄積する。EMM復号部115はKmを用いてEMMの復号を行う。ECM復号部114はEMM復号部115で取得されたKwを用いて復号を行う。ここで、先ほどEMM復号部115にて復号された契約情報とECM復号部114にて復号された番組信号とから、受信信号が受信者にとって視聴可能な信号であるかを視聴判定部117で判定し、視聴可能な信号であった場合、取得されたKsを用いてデスクランブル部113にてデスクランブルを行い出力する。これらECM復号部114、EMM復号部115、及び視聴判定部117は、CPU内蔵のICカードの中の処理プログラムとして実現されることも多い。

【0021】送信装置101から伝送された信号は、受信部112で受信する。その後、スクランブル信号は蓄積部116にスクランブルされた信号のまま蓄積される。同様にECMはECM蓄積部211に、EMMはEMM蓄積部212に夫々蓄積される。

【0022】ここで、受信者が蓄積部116にある特定の番組情報を視聴する指示をした場合、受信機111は、まずEMM復号部115が、EMM蓄積部212に蓄積されている指定された番組信号に対応したEMMを復号し、Kw及び契約情報を取得する。ECM復号部114はECM蓄積部211より受信者が指定した番組情報に対応したECMを復号し、Ks及び番組情報を取得する。EMM復号部115にて取得した契約情報とECM復号部114にて取得した番組情報とから受信者が視聴可能な番組か否かの判定を行い、視聴可能であった場合、デスクランブル部113にKsを出力する。デスクランブル出力部113は蓄積部より、受信者が指示した番組のスクランブル信号をKsを用いてデスクランブルし、出力する。

【0023】しかしながら、図2の受信システムの場合、蓄積を対象としない放送信号を蓄積した後、再生して視聴しているので、受信機111においてECM復号部114より送られるKsでは、放送された信号と同じ順序で再生されるスクランブル信号のデスクランブルは行えるが、逆の順序で再生されるスクランブル信号がデスクランブル部113に入力される前にその対応するKsを取得することができない。

【0024】

【発明が解決しようとする課題】上記のように、従来の限定受信システムでは、特殊再生処理を行うために事前にデスクランブルした信号を蓄積するシステム構成の場合、実際には視聴していない番組でも課金されてしまうという問題があった。又、視聴した番組のみ課金対象となるようなシステム構成の場合、特殊再生処理ができないという問題があった。

【0025】本発明は、上記問題点に鑑みなされたもの



であり、スクランブル方法、送信方法、送信装置、及び受信機を提供することを目的とする。

【0026】

【課題を解決するための手段】上記課題を解決するために、本件発明は、以下の特徴を有する課題を解決するための手段を採用している。

【0027】請求項1に記載された発明は、スクランブル鍵を生成する鍵生成段階と、前記鍵生成段階によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル段階と、スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成段階とを有するスクランブル方法において、前記スクランブル鍵情報生成段階において生成されたスクランブル鍵情報は、既に使用したスクランブル鍵に関するスクランブル鍵情報を有することを特徴とする。

【0028】請求項1記載の発明によれば、スクランブル信号をデスクランブルする際に、特に巻き戻し再生に必要なスクランブル鍵を容易に取得することができる。

【0029】請求項2に記載された発明は、スクランブル鍵を生成する鍵生成段階と、前記鍵生成段階によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル段階と、スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成段階とを有するスクランブル方法において、前記スクランブル鍵情報生成段階において生成されたスクランブル鍵情報は、現在の区間の信号のスクランブルに使用するスクランブル鍵と、隣接する次の区間の信号のスクランブルに使用するスクランブル鍵と、隣接する1つ前の区間の信号のスクランブルに使用するスクランブル鍵とに関する情報を少なくとも有することを特徴とする。

【0030】請求項2記載の発明によれば、スクランブル信号をデスクランブルする際に早送り、巻き戻し等の特殊再生を容易に行うことができる。

【0031】請求項3に記載された発明は、スクランブル鍵を生成する鍵生成段階と、前記鍵生成段階によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル段階とを有するスクランブル方法において、前記スクランブル段階は、スクランブル時に用いられるスクランブル鍵の更新を、信号の符号化単位に同期して行うことを特徴とする。

【0032】請求項3記載の発明によれば、例えば、早送り、巻き戻し等の特殊再生を行う場合に、符号化単位、又はその整数倍の区切りでスクランブル鍵の更新を行うことで、その区間のスクランブル鍵を明確にし、特殊再生時のデスクランブル時に容易に画像もしくは音声を表示させることができる。

【0033】請求項4に記載された発明は、請求項3記載のスクランブル方法において、前記スクランブル段階

は、スクランブル時に用いられるスクランブル鍵の更新を、符号化信号の少なくとも1つのGOP単位に同期して行うことを特徴とする。

【0034】請求項4記載の発明によれば、スクランブル信号のある区間におけるスクランブル鍵を明確にし、特殊再生時のデスクランブル時に容易に画像もしくは音声を表示させることができる。

【0035】請求項5に記載された発明は、請求項3又は4記載のスクランブル方法により生成されたスクランブル信号と暗号化されたスクランブル鍵情報とを同時に送信する送信方法において、前記スクランブル鍵情報は、符号化単位に同期して区切られた信号の切り替え点における直前もしくは直後、又はその両方に付加することを特徴とする。

【0036】請求項5記載の発明によれば、スクランブル信号をデスクランブルする際に早送り、巻き戻し等の特殊再生時にも受信者が待ち時間なく、映像信号、又は音声信号の再生を容易に行うことができる。

【0037】請求項6に記載された発明は、スクランブル鍵を生成する鍵生成部と、前記鍵生成部によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル部と、スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成部とを有する送信装置において、前記スクランブル鍵情報生成部において生成されたスクランブル鍵情報は、既に使用したスクランブル鍵に関するスクランブル鍵情報を有することを特徴とする。

【0038】請求項7に記載された発明は、スクランブル鍵を生成する鍵生成部と、前記鍵生成部によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル部と、スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成部とを有する送信装置において、前記スクランブル鍵情報生成部において生成されたスクランブル鍵情報は、現在の区間の信号のスクランブルに使用するスクランブル鍵と、隣接する次の区間の信号のスクランブルに使用するスクランブル鍵と、隣接する1つ前の区間の信号のスクランブルに使用するスクランブル鍵とに関する情報を少なくとも有することを特徴とする。

【0039】請求項8に記載された発明は、スクランブル鍵を生成する鍵生成部と、前記鍵生成部によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル部とを有する送信装置において、前記スクランブル部は、スクランブル時に用いられるスクランブル鍵の更新を、信号の符号化単位に同期して行うことを特徴とする。

【0040】請求項9に記載された発明は、請求項8記載の送信装置において、前記スクランブル部は、スクランブル時に用いられるスクランブル鍵の更新を、符号化信号の少なくとも1つのGOP単位に同期して行うこと

を特徴とする。

【0041】請求項10に記載された発明は、請求項8又は9記載の送信装置により生成されたスクランブル信号と暗号化されたスクランブル鍵情報とを同時に送信する送信装置において、前記スクランブル鍵情報は、符号化単位に同期して区切られた信号の切り替え点における直前もしくは直後、又はその両方に付加することを特徴とする。

【0042】請求項6から10に記載された発明によれば、請求項1乃至4何れか一項記載のスクランブル方法、又は請求項5の送信方法に適した送信装置を提供することができる。

【0043】請求項11に記載された発明は、スクランブル鍵によりスクランブルされた信号を受信する受信部と、スクランブル信号を蓄積する蓄積部と、スクランブル鍵情報を復号するスクランブル鍵情報復号部と、スクランブル信号をデスクランブルするデスクランブル部とを有する受信機において、前記スクランブル鍵情報復号部において復号されたデスクランブル鍵情報は、既使用したデスクランブル鍵に関するデスクランブル鍵情報を有することを特徴とする。

【0044】請求項11の発明によれば、逆方向（巻き戻し）再生を行いながら、デスクランブルを行うことができる受信機を提供することができる。

【0045】請求項12に記載された発明は、スクランブル鍵によりスクランブルされた信号を受信する受信部と、スクランブル信号を蓄積する蓄積部と、スクランブル鍵情報を復号するスクランブル鍵情報復号部と、スクランブル信号をデスクランブルするデスクランブル部とを有する受信機において、前記スクランブル鍵情報復号部において復号されたデスクランブル鍵情報は、現在の区間の信号のデスクランブルに使用するデスクランブル鍵と、隣接する次の区間の信号のデスクランブルに使用するデスクランブル鍵と、隣接する1つ前の区間の信号のデスクランブルに使用するデスクランブル鍵とに関する情報を少なくとも有することを特徴とする。

【0046】請求項12の発明によれば、早送り、巻き戻し等の特殊再生を行いながら、デスクランブルを行うことができる受信機を提供することができる。

【0047】

【発明の実施の形態】本発明は、特殊再生処理を行いながらデスクランブルを行うことができる信号のスクランブル方法、送信方法、送信装置、及び受信機を提供することを主眼とする。

【0048】本発明は、スクランブルがかかった信号のまま記録した信号に早送り、巻き戻し等の特殊再生を行う場合に、デスクランブル時に鍵の再生が間に合わないことがないよう、現在の区間に対応するスクランブル鍵K<sub>s</sub>の他に、隣接する一つ先の区間の信号のスクランブルに使用するスクランブル鍵K<sub>s\_a</sub>、隣接する一つ

前の区間の信号のスクランブルに使用するスクランブル鍵K<sub>s\_b</sub>をもスクランブルを復元するための関連情報（ECM）に記録することにより、特殊再生時にも受信者が待ち時間なく、映像信号、又は音声信号を表示できるようにする。

【0049】なお、（社）電波産業会（ARIB）の標準規格「BSデジタル放送限定受信方式」（ARIB STD-B25）によれば、ECMセクション構造にはスクランブル鍵（Odd）、スクランブル鍵（Even）があり、「現在と次の、2つのスクランブル鍵をペアで送る。」との記載があるが、一つ前のスクランブル鍵とペアで送る規格及び現在と次と一つ前の3個のスクランブル鍵が存在するECMセクション構造の規格はまだない。

【0050】また、本発明はスクランブル時に用いられるスクランブル鍵の更新を、信号の符号化単位、又は少なくとも1つのGOP（Group Of Picture）単位に同期して行うことにより、その区間のスクランブル鍵を明確にし、特殊再生時のデスクランブルを容易に行うことができる。

【0051】なお、スクランブル鍵情報においては、K<sub>s\_a</sub>及びK<sub>s\_b</sub>は、符号化単位に同期して区切られた信号の切り替え点の直前もしくは直後、又はその両方に付加することにより、次の区間までの時間が短い場合、又は高速な特殊再生を行う場合等において、次にデスクランブルされる区間に対応する鍵をより確実に再生することができる。

【0052】デジタル放送における限定受信方式は、例えば、ARIBの標準規格ARIB STD-B25に示されているように、映像信号や音声信号はデジタル符号化され、MPEG多重化方式の規格で示されるようなTSパケットのペイロード部分に載せて送られる。

【0053】信号をスクランブルして伝送する場合には、TSパケットのペイロード部分がブロック暗号方式で暗号化される。この暗号化と復号に使用されるスクランブル鍵K<sub>s</sub>は、番組情報と共に、ECMとして構成され、スクランブルされた信号と同じ伝送路で受信機に送られる。

【0054】このECMは秘密の鍵情報を含むことから、ワーク鍵K<sub>w</sub>と呼ばれる鍵で暗号化して送られる。

【0055】受信機では、まずこのECMの暗号を復号してK<sub>s</sub>を取得し、これを用いて信号のスクランブルを復元する。このとき、ECMの暗号化データの復号には時間が必要であり、この復号時間を経た後でなければ、デスクランブルすることができない。復号時間は受信機回路の性能によっても変わるので、K<sub>s</sub>を一つしか送らないシステムでは、全ての受信機で暗号化データの復号が完了した後でなければ、そのK<sub>s</sub>を用いて信号をデスクランブルすることはできず、この時間が、チャンネルを切り替えたときに番組が受信されるまでの待ち時間と

なっていた。

【0056】このため、BSデジタル放送の限定受信システム(CAS(Conditional Access System))では、一つのECMの中に奇数期間と偶数期間に使用するKsを別個に設けている。

【0057】信号の各TSパケットがいずれのKsでスクランブルされているかは、各TSパケットのヘッダ内に存在するスクランブル制御フラグの値によって識別される。

【0058】ここで、これら二つのKsによる信号のスクランブル(TSパケットのヘッダのスクランブル制御フラグの値)とECMで送るKsの時間の関係を示すと図3のようになる。

【0059】図3は、時間の経過と共に各区間で、ある特定のKsによりスクランブルされたTSパケットと各区間で送られるECM信号との関連を示した従来のスクランブル信号とECMの関連図である。

【0060】図3において、例えば区間IIに含まれるTSパケット2はKs(偶1)でスクランブルが行われ、区間IIIに含まれるTSパケット3はKs(奇2)でスクランブルが行われている。なお、時間はT1からT2へと経過していくものとする。

【0061】この信号において、デスクランブルを行うためのECMを送るTSパケットは、MPEG多重方式ではスクランブルした信号を送るTSパケットの間に時分割で多重化されて送られるが、区間IIの信号をデスクランブルするためのECMは一般的には、区間Iの開始直後すなわち時刻T1の直後に送られる。

【0062】受信機ではこのECMを受信して暗号化データの復号を行うと、Ks(偶1)とKs(奇1)が得られる。

【0063】従って、T1の直後に受信したECMを復号処理する時間が時間(T2-T1)の間隔より長くならなければ、区間IIの信号が受信される前に、Ks(偶1)が得られ、正しくデスクランブルできることになる。

【0064】このような方法をとることにより、ECMの復号処理が終了すると同時にKsによるデスクランブルが可能となる。

【0065】一方、放送の場合は番組の途中から受信することが多いので、受信を開始して最初に受信されたECMを復号したとき、Ks(奇1)が得られれば、区間Iの途中からでもデスクランブルが可能になり、T2まで待つ必要がなくなる。

【0066】この途中受信の場合の待ち時間を少なくするために、各区間の途中でも図3に示したように、その区間内でのKsとその先のKs(Ks\_a)を含むECMが伝送されるのが一般的である。

【0067】ところで、図3に示したT1→T2→T3→T4といった時間順序で番組の信号が記録された場

合、今スクランブルが行われていない視聴可能な番組信号を考えると、後に述べるように、受信機に適当な蓄積部を用意することにより、T4→T3→T2→T1といった逆方向に再生する場合に映像等を再生することが可能となる。

【0068】しかし、スクランブルが行われている信号に対し、T4→T3→T2→T1といった逆方向に再生する場合には、図3の構成では、スクランブル信号に対応するECMを取得して暗号化データを復号しても、得られるKsは逆方向に進行する区間のものであり、その次の区間のKs(Ks\_b)を取得することができず、連続的に信号をデスクランブルすることはできない。

【0069】そこで、逆方向への再生が可能となるような本発明の実施の形態を図4に示す。

【0070】図4は、本発明実施の一例の図である。

【0071】図4は図3と同様に、時間の経過と共に各区間である特定のKsによりスクランブルされた少なくとも1つのGOP(Group Of Picture)単位で生成されたTSパケットと、各区間で送られるECM信号との関連を示したものである。

【0072】図4において、順方向と逆方向(巻き戻し)のいずれの再生の場合にも利用できるようなKsを配置したECMを生成する。

【0073】例えば、区間IIで再生されたECMの暗号を復号すると、その区間に使用されているKs(偶1)と共に、Ks(奇2)とKs(奇1)が得られる。

【0074】ここで、図4の各区間で送られるECM内の鍵において、上部に記載されているKsを現区間のTSパケットを再生する場合のKsとし、中部に記載のKsを順方向再生の場合に使用するKsとし、下部に記載のKsを逆方向再生の場合に使用するKsとする。

【0075】例えば、区間IIで再生されたECMの暗号を復号すると、その区間に使用されているKs(偶1)と共に、Ks(奇2)とKs(奇1)が得られる。

【0076】Ks(奇2)は順方向再生の場合に使用し、Ks(奇1)は逆方向再生の場合に使用する。従って、区間IIの後に区間Iの信号が再生されても、Ks(奇1)を用いて正しくデスクランブルすることができる。

【0077】なお、順方向の早送りや巻き戻しで高速に再生する場合には、区間の時間長とECMの暗号、復号に要する時間の比に対応する速度比までが正しくデスクランブルできる範囲となる。

【0078】次に、特殊再生と信号のTSパケットの関係について述べる。ここで、信号として映像信号を考えると、デジタル放送等で多く使用されているMPEG-2の画像符号化方式ではフレーム内符号化、フレーム間予測符号化が組み合わされており、フレーム内符号化を行うフレームをIピクチャという。また、フレーム間予測符号化では、順方向予測による符号化を行うフレーム

をPピクチャといい、両方向予測による符号化を行うフレームをBピクチャという。前記のピクチャタイプにより画像フレームが組み合わされている。これらはGOP (Group Of Picture) と呼ばれる単位 (例えば0.5秒間の映像に対応) で処理されるのが一般的である。

【0079】いま、記録された映像信号を逆方向で再生して、受信者が認識可能な画像を再現する場合には、例えば、GOP単位又はその整数倍の画像に対応する分のTSパケットをまとめてバッファメモリ等に記録して、逆方向再生等の処理を行うのが適当である。

【0080】この点から、映像信号をスクランブルする場合のKsは、この画像符号化の単位に関連した区間で更新することが適当であるといえる。

【0081】また、本発明は、スクランブルを行うKsの奇数、偶数を切り替える時点を、画像符号化の適当な単位の境界とする方法と装置を与えるものである。この切替えの単位としては、例えば、前述のGOP単位あるいは複数のGOP単位とするのが適当である。

【0082】記録された信号を早送り等の高速で再生する場合に映像等を出力するには、バッファメモリ等に記録した後、処理を行って出力するが、高速で再生されるので、一部の映像信号と音声信号を抽出して提示することになる。

【0083】このとき、信号にスクランブルが行われている場合には、デスクランブルを行った上で処理する必要がある。

【0084】なお、MPEG-2の画像符号化方式と多重化方式では、符号化された各ピクチャはPES (Pack etized Elementary Stream) パケットと呼ばれるパケットに構成され、これを分割してTSパケットのペイロード部分に入れて伝送、あるいは記録されるが、MPEGの規格では一つのTSパケットに複数のPESパケットの信号が入ることはないので、TSパケットのスクランブル鍵Ksを確実に区別することができる。

【0085】なお、本発明の説明で、各区間で送られるECM内のKsの数を3つとしたが、付与できる数は、この限りではない。

【0086】ここで、本発明を使用した実施例を図面を用いて説明する。

【0087】図5は、本発明を使用した限定受信システムの一構成例である。

【0088】図5において、本発明を使用した限定受信システムは送信装置101、受信機111より構成されている。送信装置101は、スクランブル部102、Ks生成部503、ECM生成部504、Kw生成部105、EMM生成部106、送信部107より構成されている。また、受信機111は、受信部112、デスクランブル部113、ECM復号部514、EMM復号部115、蓄積部116、視聴判定部117、ECM蓄積部211、EMM蓄積部212より構成されている。

【0089】送信装置101に番組信号が入力されると、スクランブル部102とKs生成部503に入力される。Ks生成部503はTSパケットに対してKsを生成し、スクランブル部102に出力する。スクランブル部102は、番組信号をKsを用いてスクランブルを行う。

【0090】Ks生成部503は、ECM生成部504に対し、現在のTSパケット信号に対するスクランブル鍵Ksの他に、時間的に未来に位置する隣接したTSパケット信号のスクランブル鍵Ks\_aと時間的に過去に位置する隣接したTSパケット信号のスクランブル鍵Ks\_bとを出力する。ECM生成部504は、Ks、Ks\_a、Ks\_bと番組情報をKw生成部105から入力されるKwを用いて暗号化しECMを生成する。Kw生成部105は、ECM生成部に出力したKwと同一のKwをEMM生成部106に出力する。EMM生成装置106では、Kwと契約情報からKmを用いて暗号化しEMMを生成する。送信部107は、スクランブル信号、ECM、EMMを送信する。

【0091】送信装置101から伝送されたスクランブル信号、ECM、EMMは受信部112で受信されると、スクランブル信号は蓄積部116にスクランブル信号のまま蓄積される。ECMはECM蓄積部211に、EMMはEMM蓄積部212に蓄積される。その後、EMM復号部115でマスタ鍵を用いてEMM信号を復号し、Kw及び契約情報を取得する。ECM復号部514では、復号したKwを用いてECM信号の復号を行い、Ks、Ks\_a、Ks\_b、及び番組情報を取得する。

【0092】次に、蓄積部116に蓄積しているスクランブルされた番組の再生方法を選択する。再生方法には、通常再生の他に、早送り再生、巻き戻し再生等の特殊再生が存在する。視聴判定部117は、EMM復号部115で復号された契約情報、及びECM復号部514で復号された番組情報から、選択されたスクランブル信号が受信者との契約上視聴可能であるかを判定し、視聴可能であった場合、選択された再生方法に従い、その対応したスクランブル鍵をデスクランブル部113に送る。デスクランブル部113は、指示された再生方法に従ってデスクランブルを行い出力する。

【0093】前記から送信装置101、及び受信機111を使用することにより、受信者が視聴を希望した番組のみにデスクランブルを行うことができ、さらに、早送り、巻き戻し等の特殊再生を行うことができる。

【0094】本発明を利用することにより、例えば、CATV等のケーブル伝送路を介して、放送局側のビデオサーバーから希望の映画等の番組にスクランブルをかけて配信する場合に、受信側からの操作で画面を確認しながら巻き戻すといった特殊再生を行うことができるようになる。このシステム構成が、単純にサーバーにはスクランブルされていない信号を蓄積し、再生した後でスク

ランブルを行って伝送する場合には、従来の技術において実現できるが、その場合、受信する人の数だけスクランブラが必要になり、放送のような多数の受信者を対象とするシステムでは現実的ではない。

【0095】従って、スクランブルされた信号をサーバに記録しておき、この再生の制御のみを受信者ごとに行えるようにするシステムが好適であるといえる。

【0096】本発明を実施することにより、スクランブルされて伝送された信号を特殊再生しながら、デスクランブルして視聴することができる。

【0097】

【発明の効果】本発明は、特殊再生処理を行いながら、デスクランブルを行うことができる信号のスクランブル方法、送信方法、送信装置、及び受信機を提供することができる。

【図面の簡単な説明】

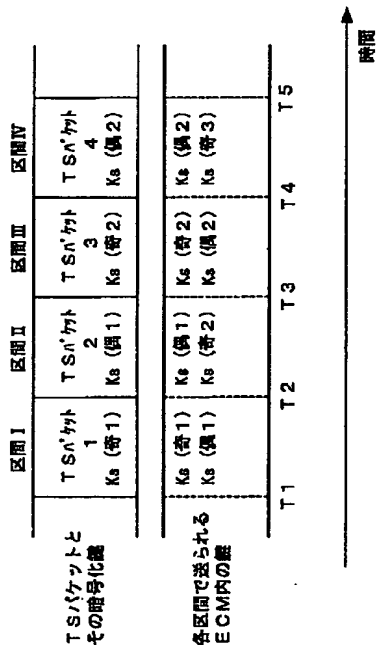
【図1】従来の限定受信システムの第一の構成例である。

【図2】従来の限定受信システムの第二の構成例である。

【図3】従来のスクランブル信号とECMの関連図である。

【図3】

従来のスクランブル信号とECMの関連図



る。

【図4】本発明実施の一例の図である。

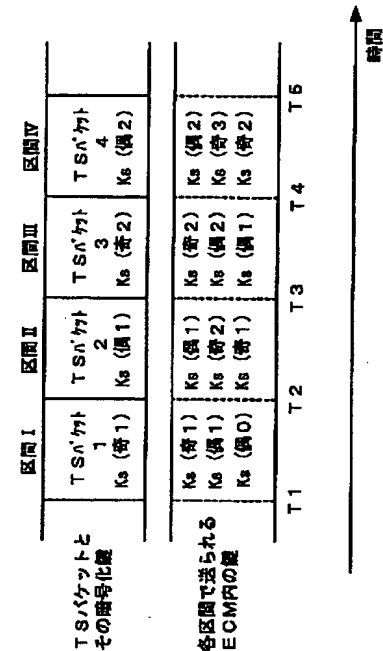
【図5】本発明を使用した限定受信システムの一構成例である。

【符号の説明】

- 101 送信装置
- 102 スクリンブル部
- 103、503 Ks生成部
- 104、504 ECM生成部
- 105 Kw生成部
- 106 EMM生成部
- 107 送信部
- 111 受信機
- 112 受信部
- 113 デスクランブル部
- 114、514 ECM復号部
- 115 EMM復号部
- 116 蓄積部
- 117 視聴判定部
- 20 211 ECM蓄積部
- 212 EMM蓄積部

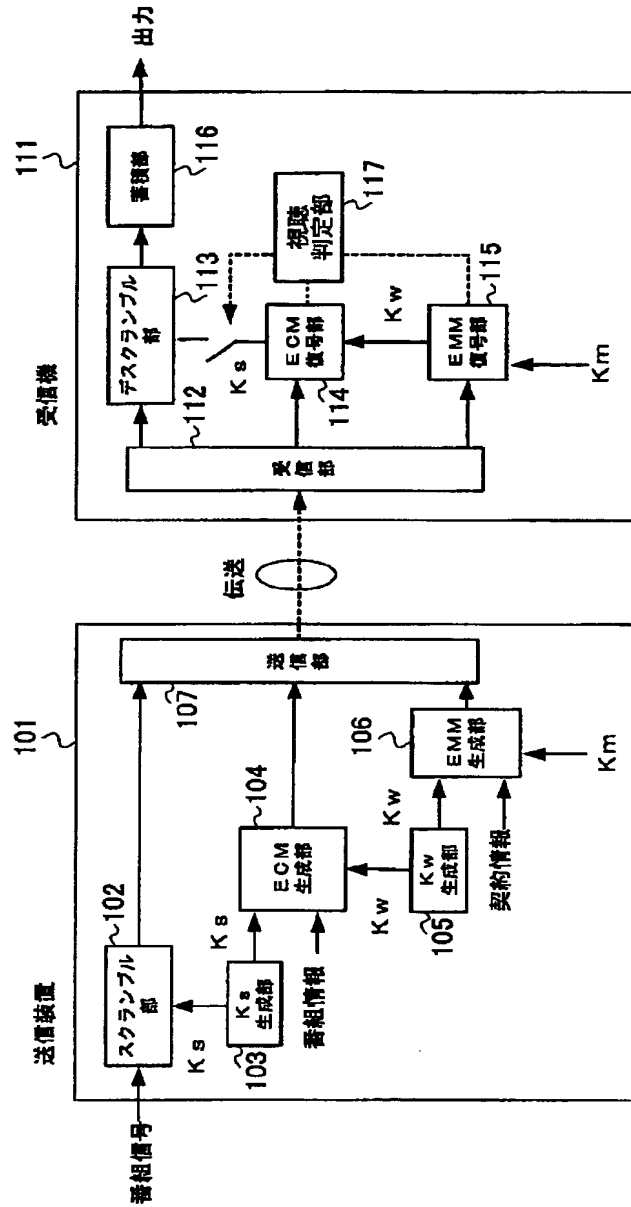
【図4】

本発明実施の一例の図



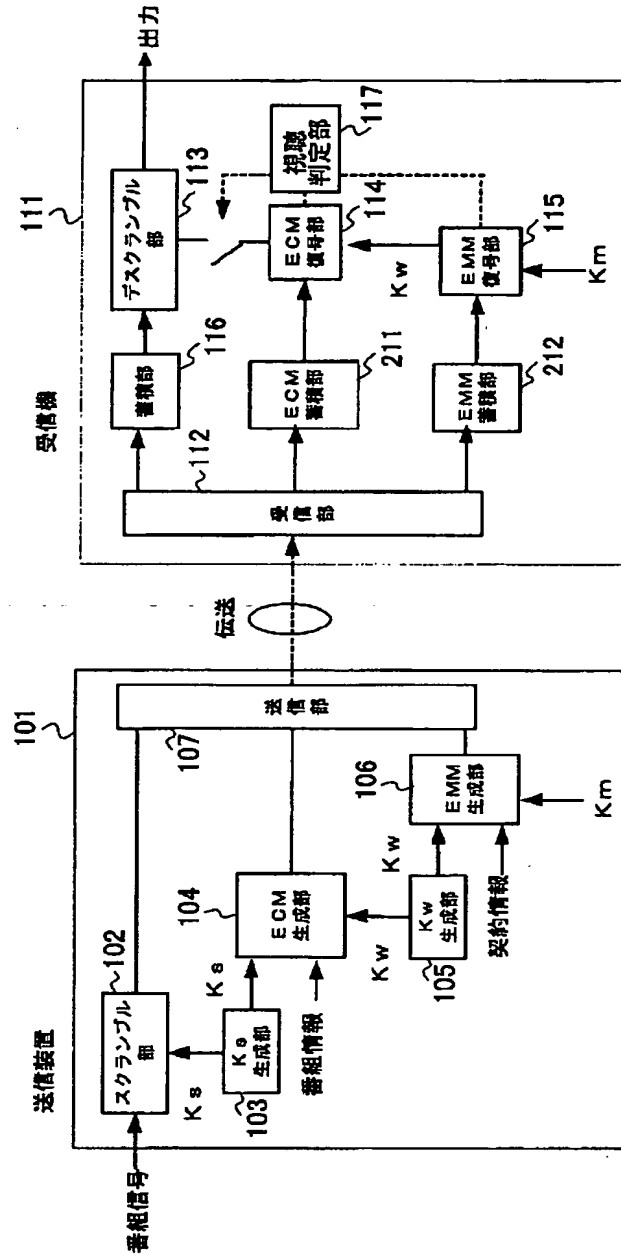
【図1】

## 従来の限定受信システムの第一の構成例



【図2】

## 従来の限定受信システムの第二の構成例



【図5】

## 本発明を使用した限定受信システムの一構成例

